# Attacks on Implementations of Secure Systems

July 14, 2019

# Chapter 1

# Introduction

Once upon a time... This document shows how you can get ePub-like formatting in LaTeX with the `memoir` document class. You can't yet export directly to ePub from writeLaTeX, but you can download the source and run it through a format conversion tool, such as `htlatex` to get HTML, and then go from HTML to ePub with a tool like Sigil or Calibre. See `http://tex.stackexchange.com/questions/16569` for more advice. And they lived happily ever after.

# Contents

# Chapter 2

# Writing LaTeX

## 2.1 Basic Formatting

**Comments.** If you want to just add a comment to a file without it being printed, add a `%` (percentage) sign in front of it. In the template files, you will find a number of such comments as well as deactivated commands.

**Bold formatting.** You can make your text bold by surrounding it with the command `\textbf{}`.

**Italics formatting.** You can make your text italic by surrounding it with the command `\textit{}`.

**Small caps.** You can change your text into small capitals by surrounding it with the command `\textsc{}`.

**Text em dashes.** Em dashes are used to connect two related sentences. There is no space before or after the em dash. Within the template, use the command `\textemdash{}` instead of using the dash you copied over from your text file. This will also take care of issues relating to line breaks.

**Paragraphs.** Paragraphs are handled automatically by leaving an empty line between each paragraph. Adding more than one empty line will not change anything—remember it is not a "what you see is what you get" editor.

**Empty line.** If you want to force an empty line (recommended only in special cases), you can use `~\\` (tilde followed by two backslashes).

**New page.** Pages are handled automatically by LaTeX. It tries to be smart in terms of positioning paragraphs and pictures. Sometimes it is necessary to add a page break, though (ideally, at the very end when polishing the final text). For that, simply add a `\newpage`.

**Quotation marks.** In the normal computer character set, there are more than one type of quotation marks. It

is required to change all quotation marks into ``...'' (two back ticks at the beginning and two single ticks at the end) and refrain from using "..." (or "...") altogether. This is because Word's "..." uses special characters, and "..." do not mark the beginning and end of the quotation.

**Horizontal line.** For a horizontal line, simply write `\hline`.

**Underlined text.** It is generally not recommended to use underlined text.

**URLs.** For URLs you need a special monospaced font. Also, for URLs in e-books, you want to make them clickable. Both can be accomplished by putting the URL in the `\url{}` environment, for example `\url{https://www.lode.de}`.

**Special characters.** If you need special characters or mathematical formulas, there is a whole body of work on that subject. It is not in the scope of this book to provide you a comprehensive list.

## 2.2 Lists

**Itemized list.** To create a bullet point list (like the list in this section), use the following construct:

```
\begin{itemize}
    \item Your first item.
    \item Your second item.
    \item Your third item.
%   \item Your commented item.
\end{itemize}
```

The result will look like this:

- Your first item.
- Your second item.
- Your third item.

**Numbered list.** To create a numbered list, replace itemize with enumerate:

```
\begin{enumerate}
    \item Your first item.
    \item Your second item.
    \item Your third item.
\end{enumerate}
```

The result will look like this:

1. Your first item.

2. Your second item.

3. Your third item.

## 2.3 Verbatim text

Sometimes, you do want to simply use text in a verbatim way (including special characters and LaTeX commands). For this, simply use the `\lstlisting` environment: `\begin{lstlisting}...\end{lstlisting}`. For example, I put the itemize and enumerate listings above into a `\lstlisting` block. If I did not, LaTeX would have displayed the list as a list, instead of displaying the code.

## 2.4 Chapters and Sections

LaTeX uses a hierarchy of chapters, sections, and subsections. There are also sub-subsections, but for the sake of the reader, it is best to not go that deep. If you come across a situation where it looks like you need it anyway, I recommend thinking over the structure of your book rather than using sub-subsections.

In terms of their use in the code, they are all similar:

- `\chapter{Title of the Chapter}\label{c1_chaptername:cha}`

- `\section{Title of the Section}\label{c1_sectionname:sec}`
- `\subsection{Title of the Subsection}\label{c1_subsectionname:sec}`
- `\paragraph{Title of the Paragraph}\label{c1_paragraph:sec}`

When using these commands, obviously replace the title, but also the label. For the label, I recommend to have it start with c, followed with the current chapter number, an underscore, and the chapter, section, or subsection in one word and lowercase, followed by either ":cha" or ":sec" to specify what kind of label it is. These labels can then be used for references like we used previously for the images. For example, if you have defined a section `\section{Chapters and Sections}\label{c1_chaptersandsections:sec}`, you could write "We will discuss chapters and sections in section `\ref{c1_chaptersandsections:sec}` which results in the document in "We will discuss chapters and sections in section 2.4".

## 2.5 Tables

In LaTeX, tables are like images and put into the figure environment. As such, they have a caption, label, and

a positioning like we discussed above with the images. Drawing a table requires a bit of coding:

```
\begin{table}[!ht]
    \centering
    \begin{tabular}{p{2.5cm}|p{3.5cm}|p{3.5cm}}
    \hline
    & \textbf{Word} & \textbf{\LaTeX{}} \\
    \hline

    Editor & ``what you see is what you get'' & source file is compiled \\
    \hline

    Compatibility & dependent on editor & independent of editor \\
    \hline

    Graphics & simple inbuilt editor & powerful but complex editor \\
    \hline

    Typography & optimized for speed & optimized for quality \\
    \hline
```

```
19
20      Style & inbuilt style & separate↩
            style document \\
21      \hline
22
23      Multi-platform & only via export↩
            & possible with scripting \\
24      \hline
25
26      Refresh & some elements need, ↩
           manual refresh & everything ↩
           is refreshed with each ↩
           compile \\
27      \hline
28
29      Formulas & basic support needs ↩
           external tools & complete ↩
           support \\
30      \hline
31
32      \end{tabular}
33      \caption{Comparison of Word and ↩
           \LaTeX{}} \label{c1_↩
           comparisonwordlatex:tab}
34  \end{table}
```

This table from the beginning of the book has the familiar figure, label, caption, and centering commands. The actual table is configured with the `\tabular{}` envi-

ronment. Following the tabular command, you configure the columns in curly braces. Each column is separated with a vertical line and the `p{...}` entry specifies the width of the column. With `{p{2.5cm}|p{3.5cm}|p{3.5cm}}`, you would have three columns with 2.5cm width for the first column and 3.5cm width for the two others. Alternatively, you can use `c` instead of `p` and leave out the curly braces with the width. Then, LaTeX simply calculates the required widths automatically. Then, for each line of the table, simply write: `content of the first cell & content of the second cell & content of the third cell\\\hline`.

## 2.6 Footnotes

Finally, for footnotes, there is the command `\footnote{}`. You can place it anywhere you like, LaTeX will then automatically add the number of the footnote at that place, and put the footnote text into the footer area. It looks like this.[1] The challenge here relates to grammar: footnotes start with capital letters, parentheses with lower case, and the footnote comes after the period, the parentheses have to start before the period.

[1] This is a footnote.

| | **Word** | **LaTeX** |
|---|---|---|
| Editor | "what you see is what you get" | source file is compiled |
| Compatibility | dependent on editor | independent of editor |
| Graphics | simple inbuilt editor | powerful but complex editor |
| Typography | optimized for speed | optimized for quality |
| Style | inbuilt style | separate style document |
| Multi-platform | only via export | possible with scripting |
| Refresh | some elements need, manual refresh | everything is refreshed with each compile |
| Formulas | basic support needs external tools | complete support |

Table 2.1: Comparison of Word and LaTeX

# Chapter 3

# Inserting Images

## 3.1 Images

As in Word, in LaTeX, images are separate from the text. Images are usually packaged together with a caption and a label to reference it from the text. These three entities are packaged together into a figure. The figure itself configures the size of the image as well as where it should be put. Let us look at a code sample:

```
1  \begin{figure}[H]
2      \centering
3      \includegraphics{images/↩
           ebookLatex_Cover.jpg}
4      \caption{The cover of this book↩
           .} \label{c1_cover:fig}
5  \end{figure}
```

Let us go through this line by line. At the core is the image, included with `\includegraphics{path to file}`. It inserts the image specified by the "path to file." With the `\adjustbox{}` command, we can adjust the image size according to the page width (`\columnwidth`) and page height (`\textheight`).

Below there is the caption and the label. LaTeX automatically numbers each figure, so in the text, we can later refer to it with `\ref{c1_cover:fig}` which prints out the number of the figure. Finally, all these commands are centered with the `\centering` command and surrounded with the figure environment. The `[ht]!` instructs LaTeX to try to place the image exactly where it is in the LaTeX code.

In Figure 3.1, you can see the result of the command. Instead of graphics, you can also include other TEX files that contain graphics (or commands to draw graphics, see chapter 3.2).

## 3.2 TikZ Graphics

For graphics, you can use the inbuilt TikZ graphics generator. Due to its flexibility, I even recommend images you already have for a number of reasons:


Figure 3.1: The cover of this book.

- TikZ graphics can very easily changed (especially for for example translations or making corrections).
- TikZ graphics are small and flexible. They can be

easily scaled to any size and are directly integrated into your project (no time-consuming editing in an external graphics program necessary).

- TikZ graphics look better. As vector graphics are sent directly to the printer, we need not to worry about readability.

If you want to create a TikZ graphic, simply create a new TEX file in the *tex-images* folder and include it with `\input` (replacing `\includegraphics{}`) where you want to.

Then, do a "recompile from scratch" by clicking on the top right corner of the preview window (showing Warning or Error) to regenerate the TikZ file. If "up-to-date and saved" is shown, delete the *tikz-cache* directory and recreate it.

For the format of the file itself, it is a series of commands surrounded by the `\begin{tikzpicture}...\end{tikzpicture}` environment. Discussing all the commands is beyond the scope of this book, so I recommend three options:

- Check out the PGF manual at `https://www.ctan.org/pkg/pgf`. It is more than 1100 pages full with documentation of each command and corresponding examples.

- Check out the few example TikZ pictures from my two books [1] and [2] in the *tex-images* directory.

# Chapter 4

# Replace with Third Chapter Name

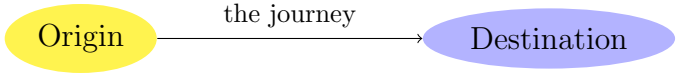


Figure 4.1: TikZ drawings will be output as SVG, which should be rendered by most modern browsers.

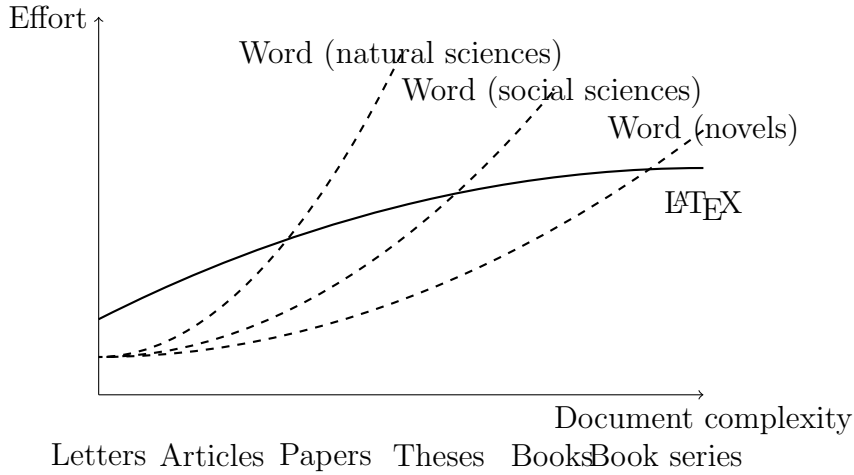


Figure 4.2: Comparing complexity of *Word* and LaTeX depending on the application.

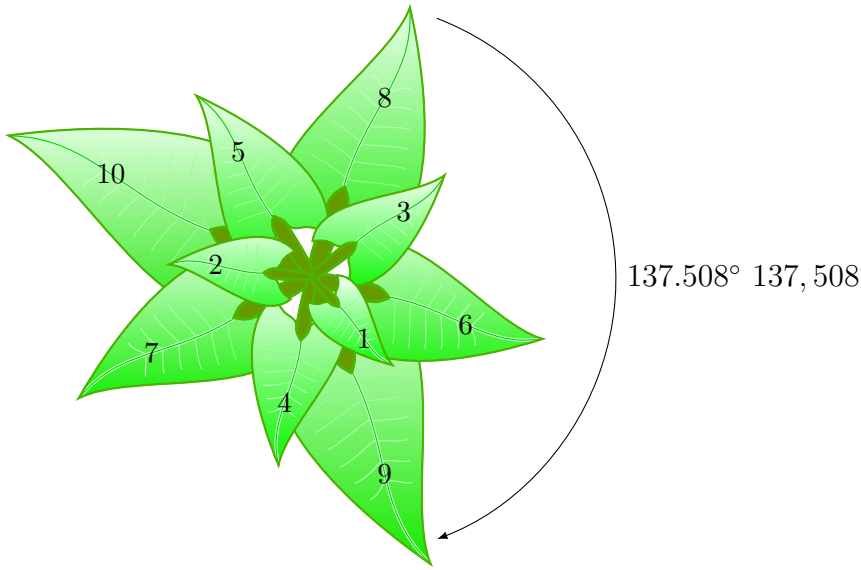


Figure 4.3: Example of a drawing made in TikZ.

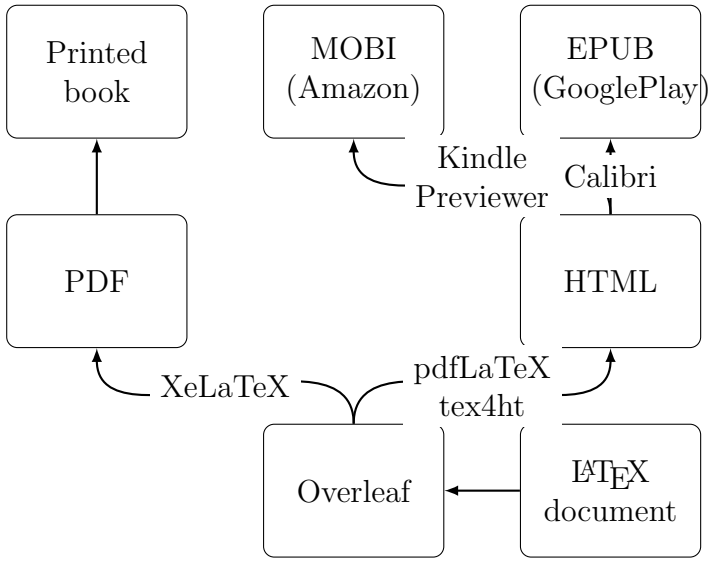


Figure 4.4: Example 2 of a drawing made in TikZ.

# Chapter 5

# Power/EM I

## 5.1 Electronic Circuits

### A basic electronic circuit

The most basic electronic circuit consist of a power supply (i.e. a battery) that generates an electric potential that aim to move to the ground. And an electrical load (any component consuming electric power) connected to the power supply (Vdd) on one side and to the "ground" (the reference point from which voltages are measured) on the other side. As the electric potential goes through the load, it (the load) does some kind of a work. We can consider electric current to behave like water, in this example the water wants to go from the mountains (Vdd) to the sea level (Ground) and there are rivers and obstacles

that tries to prevent it to do so. When the load has small resistance then more of the current will "flow" through it, and when the load has bigger resistance then the "flow" is smaller. There are two different ways in which we can wire things together in an electric circuit, called series and parallel. When things are wired in series, things are wired one after another, such that electricity has to pass through one load, then the next load, then the next, and so on. When things are wired in parallel, they are wired side by side, such that electricity passes through all of them at the same time, from one common point to another common point. The difference in the electric potential between the power supply and the ground creates an electric current which flows through the load toward the ground. The difference in electric potential between two points is measured in Volts (usually denoted by $\boldsymbol{V}$). The amount of current flowing thru the circuit at a given time is measured in Amperes (denoted by $\boldsymbol{A}$). The electrical resistance of the load is a measure of its opposition to the flow of electric current through it. It is measured in Ohms (and denoted by $\boldsymbol{R}$).

$$V = I * R$$

## Resistors

As the name implies, a resistor resists the flow of electrical current. The amount of resistance is measured in

Ohms. A resistor is considered a passive component that consumes power that is dissipated as heat. The power rating of a resistor determines how much power it can consume without overheating.

Figure 5.1: Resistor Notation.

## Ohm's law

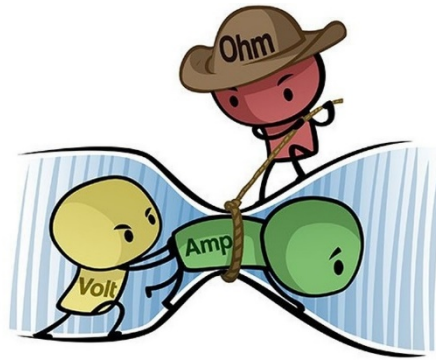


Figure 5.2: Ohm's Law.

Ohm's law defines the relationship between the Voltage, Current and Resistance in a circuit: The voltage is equal to the current multiplied by the resistance of the load. Since in most of the circuits we are using, the voltage is fixed (defined by the characteristics of the power supply), a change in the resistance of the circuit will cause a change in the current in the opposite direction. This means we can measure the current over time in order to calculate the resistance. A useful analogy for the relations between V, I and R is to imagine a fountain on a high mountain, where the water flow down through a river to the sea. The difference in height between the fountain and the sea is the Voltage, the width of the river can be thought of as the resistance, and the flow of the water is the current.

## Power

Power is the rate at which work is done by the circuit and is measured in Watts. Electricity bills are measured by K Watts hour, i.e. 1 KWH is 1 kilo watts used over an hour, and this is the energy that we used and we need to pay for. $Power = Work/Time$

Power consumption: $P = I * V$

For example we can take a look on a phone; the battery can be measure in Milliamper hour, i.e. if the battery is

3000mil Amper Hour so if the current is 1 Amper then we can use it for 3 hours. If we want the battery to run out quickly, we can use services like streaming, flashlight and more. That means we have greater current that caused by leveraging the load of the phone and the battery will run our much faster than before. The phone also, will get hot. If a device is getting hot then it sometimes uses its fans (noise), and so we can detect it for cyber usage. Electricity can be used to do various kinds of work:

- Electromagnetic work (light a bulb, transmit a WiFi signal)
- Thermal work (heating)
- Mechanical work (spin a motor, vibrate a speaker)
- Chemical work (charging a battery)
- Computational work (store or load from memory, compute a value)

## Power Consumption

When the current leaves the circuit to the ground then we consume it as power, but sometimes we need to be careful as there are cases where the current is no leaving the circuit, like battery charging. In order to measure the power we will connect our measuring device between the load and the ground. The power consumption of a

device is the work it does divided by time. It is measured in Watts ( $\boldsymbol{W}$ ). The power consumption can be calculated as current ( $\boldsymbol{I}$ ) multiplied by Voltage ( $\boldsymbol{V}$ ).

## Current and Voltage dividers

Before we take a look at two simple electronic circuits, we need to introduce two additional terms: A **short (closed) circuit** is a piece of wire with almost no resistance at all. The circuit is in a closed state and there is current in the circuit. In other words, it works as normal. An **open circuit** is a circuit which doesn't allow any current to pass through it. The circuit is in an open state and there is no current in the circuit; that's to say. It doesn't work.

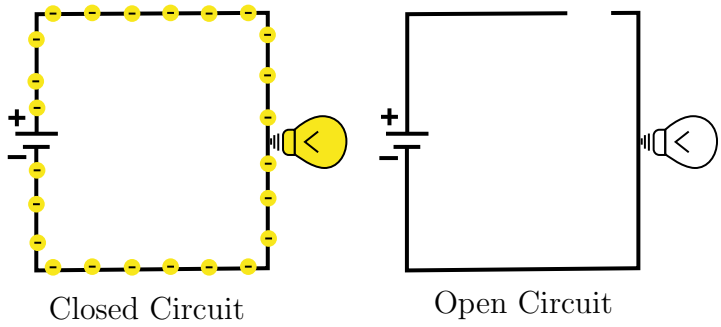


Figure 5.3: Open and closed circuits.

### Connecting in serial

If we connect a short circuit between the load and the ground (See Figure 5.4), it will have no influence on it the current will not change as from the power supply point of view – nothing has been change, we just cut a cable and put another one instead. The voltage drop will be very very low.

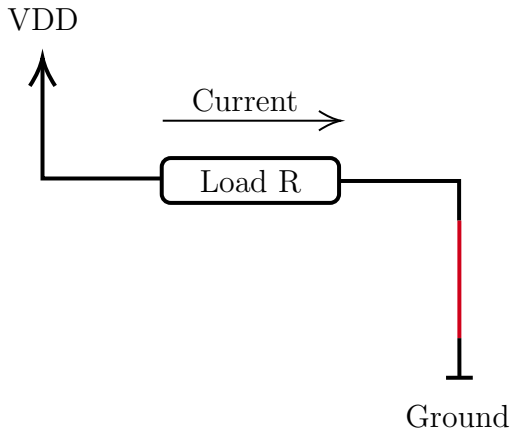


Figure 5.4: short(low resistance) circuit between the load and the ground.

If we connect an open circuit after the load (See Figure 5.5), it will increase the resistance to a very high value, causing the current to become zero effectively. If the

current is zero then the voltage is also zero (Ohm's Law).

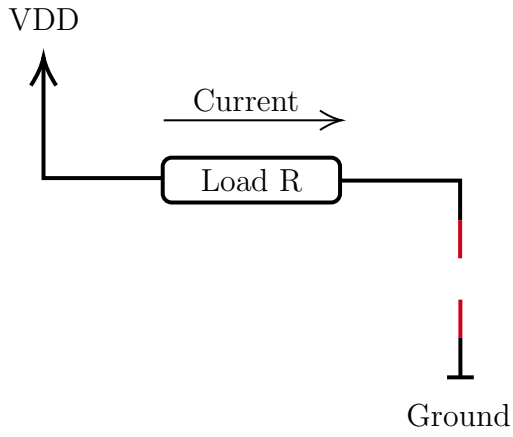


Figure 5.5: open circuit after the load.

### Connecting in parallel

If we connect an open circuit in parallel to the load (See Figure 5.6), the current will flow only thru the load path, so the current on the open circuit will be 0. However, the voltage drop between both points of the open circuit will be the same as the drop between the load sides.

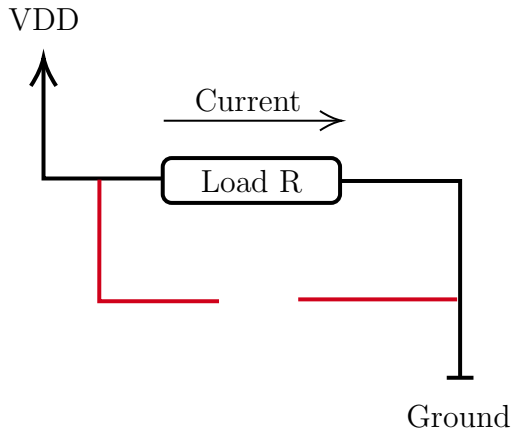


Figure 5.6: close circuit in parallel to the load.

If we connect a short circuit in parallel to the load (See Figure 5.7), the current will "prefer" flowing thru it rather than thru the load, so the current thru the load will be equal to zero, while the current thru the short circuit will be very high - by Ohm's law.

Since the cable is not a perfect conductor, some of the energy will be consumes in the form of thermal work, so the cable will heat, and possibly melt and start a fire.

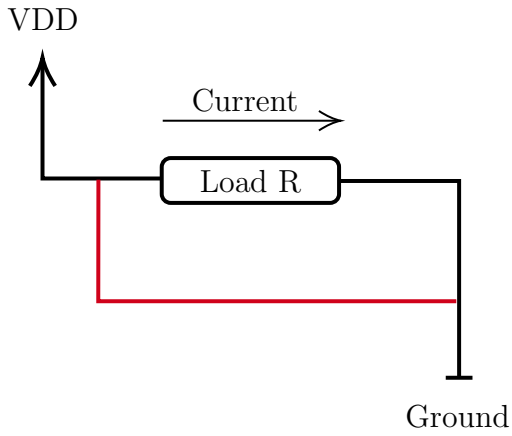


Figure 5.7: a short circuit in parallel to the load.

## 5.2 Measuring Power Consumption

Next, as an attackers, we want to measure the power consumption of this load, and to do so, we are going to use Ampermeter device.

### Ampermeter

An Ampermeter (from **Am**pere **Meter**) is a device capable of measuring the amount of electric current going through it. It has very low resistance, so it doesn't inter-

rupt the system connected to it.

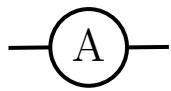


Figure 5.8: Ampermeter notation.

### Using Ampermeter to measure power consumption

We need to "cut" the wire connected to the load and connect both sides to the Ampermeter.(See Figure 5.9)
Doing so will cause all current flowing through the load to pass through the Ampermeter as well, so we will be able to read the current at any given time. The resistance of the Ampermeter is very low so it will not affect the voltage that going through the load that will have the same voltage drop as before.
Now we will measure the current going through the ampermeter and next we will convert the current in order to find the power consumption of the load.
In case we know the voltage (i.e. a 5V battery, a 220V power socket), we can compute the power consumption: $P = I * V$.
The problem: sometimes, we don't want (or simply can't) cut the circuit after the load in order to connect an Ampermeter, and this is a way that the architect of the de-

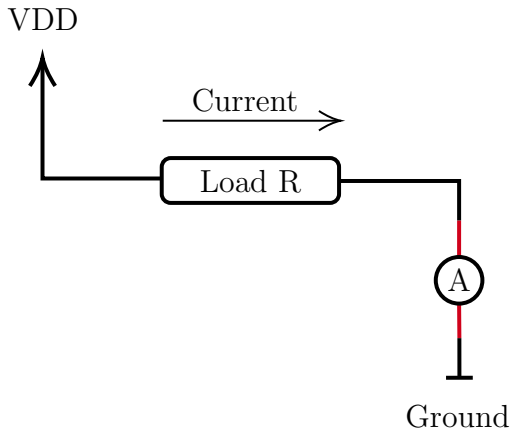


Figure 5.9: an Ampermeter connected in serial.

vice are trying to protect it. So, let's see if we can use the ampermeter without cutting anything, and let's connect it in parallel to the load. (See Figure 5.10)

Connecting the ampermeter this way will burn the ampermeter as it has no resistance and so, all of the current will flow through it. So, instead of ampermeter we can use a voltmeter as follows: (See Figure 5.11)

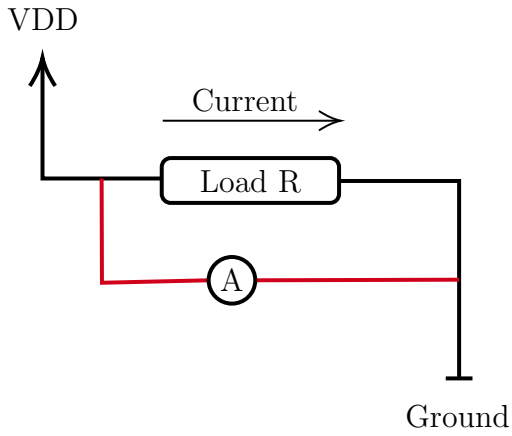


Figure 5.10: an ampermeter connected in parallel to the load

## Voltmeter

The voltmeter resistance is very very high so the current will not go through it. The voltmeter is measuring the voltage drop between one side of the load and the other side of it. If we want to measure the current using the voltmeter we are taking a load with a very small resistance and connect it as follows: (See Figure 5.12)

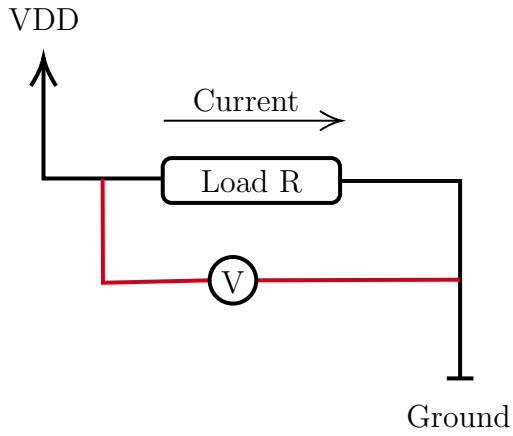


Figure 5.11: a voltmeter connected in parallel to the load

This way, because of the current divider, by connecting a Voltmeter in parallel with a very small and accurate resistor, we can measure the electric current by Ohm's law: $I = V/R$

Summary: we learnt what is Power Consumption and how we can measure it. A very important fact is that **Power Consumption varies with time!**. If we can find a relationship between the secret information we want to extract and the power consumption, we can recover this information by measuring the power consumption over time.

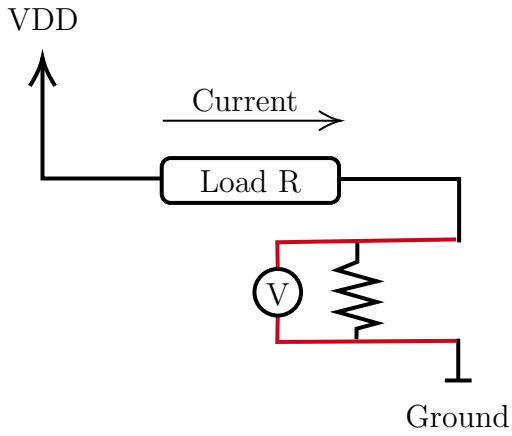


Figure 5.12: Circuit 8.

## Types of electronic components

In general there are two types of elements in the circuit, the first one are Passive devices like a resistors (a passive two-terminal electrical component that implements electrical resistance as a circuit element), inductors (is a passive two-terminal electrical component that stores energy in a magnetic field when electric current flows through it), capacitors and diodes. And there are Active devices like transistors (a semiconductor device used to amplify or switch electronic signals and electrical power), amplifiers (an electronic device that can increase the power of a signal (a time-varying voltage or current)) and ICs. From

our perspective, the Active devices are much more interesting for us (attackers) as they are using electricity in order to control electricity. One example can be an amplifier that has audio signal and power supply as inputs and it generates a greater audio signal as an output using the power supply. Another interesting active element for this course is a transistor. In an integrated circuits, there are a lot of active devices such as transistors that if we can analyze their behavior we can learn about the data that they are processing. So when we look at the final consumption of these active elements, we can figure out some kind of secrets. There are many kind of transistors and we will concentrate on understanding a certain type called Field-Effect Transistor.

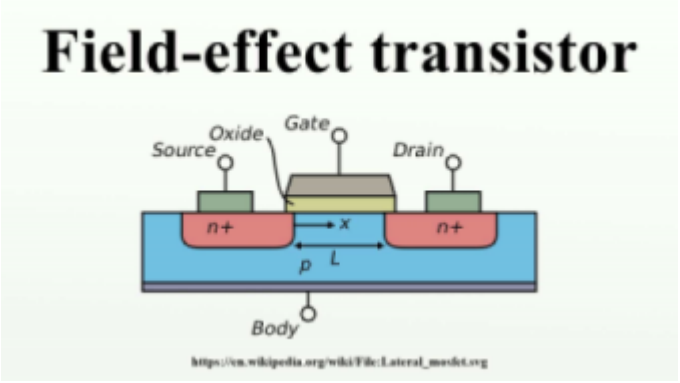


Figure 5.13: Field-Effect Transistor.

## Field-Effect Transistor

The field-effect transistor (FET) is an electronic device which uses an electric field to control the flow of current. FETs are 3-terminalled devices, having a source, gate, and drain terminal. FETs control the flow of current by the application of a voltage to the gate terminal, which in turn alters the conductivity between the drain and source terminals. In order to understand FET first we need to dive into the basics of semiconductors.

## Semiconductors

A semiconductor is a substance, usually a solid chemical element or compound, that can conduct electricity under some conditions but not others, making it a good medium for the control of electrical current. Its conductance varies depending on the current or voltage applied to a control electrode, or on the intensity of irradiation by infrared (IR), visible light, ultraviolet (UV), or X rays. In general, transistors are made of semiconducting materials such as silicon. There are a conductor like copper or gold and there are insulators like plastic or glass. Silicon atom has three parts: neutrons (not relevant for our use), protons with the positive charge (heavy) and electrons that have the negative charge and they are small and dynamic. Silicon atom has four electrons in its outer orbital and when we have a crystal silicon those 4 electrons

are set in place very nicely. It means that pure silicon is a very bad conductor as conducting means that the electrons can move around and in this case they are very comfortable where they are. Metals can be good conductors of electricity as they have "free electrons" that can move easily from atom to atom, the electricity involves the flow of electrons. As all of the outer electrons in Silicon crystal are involved in perfect covalent bonds, they cannot move around. So, silicon crystal is nearly insulator and very little electricity will flow through it. We can change the behavior of the silicon and turn it into a conductor by doping it. In doping, we mix a small amount of an impurity into the silicon crystal.
There are two types of impurities:
• N-type – where phosphorus or arsenic is added to the silicon in small quantities. They both have five outer electrons, so one of them is out of place when they get into the silicon lattice. While having nothing to bond to, the fifth electron is free to move around. As electrons have a negative charge, this kind of impurity called N-type.
• P-type - where boron or gallium is added to the silicon. They both have only three outer electrons. So, when we mixed them into the silicon lattice, there will be "holes" in the lattice where a silicon electron has nothing to bond to. The hole is looking for an electron from a neighbor atom and when that's happens the hole is "moving". As the absence of an electron creates the effect of a positive

charge, this kind of impurity called P-type.

## How does Field-Effect Transistor work?

In the Field-Effect Transistor there are (as shown in figure ..) n+ areas (N-type) and P area (P-type). The n+ area contains a lot of free electrons and the P area contains a lot of 'holes'. When no electricity is connected to the gate, the free electrons from the N+ are moving to the holes so there are no free electrons within the semiconductor itself. That means electrons can't move from the source to the drain i.e. open circuit. When electricity is connected to the gate it charge a lot of free electrons to it. The free electrons in the gate can't move to the silicon itself as there is an oxide layer between them, but is pushes the electrons in the silicon down to the body in a way there are holes between the source and the drain. That way electrons can move from the source to the drain freely and we have close circuit.

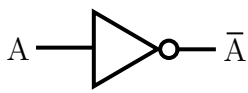


Figure 5.14: NOT Gate.

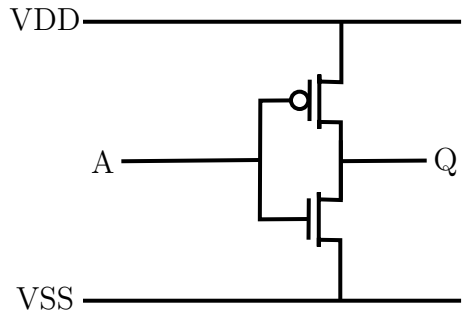


Figure 5.15: Circuit 9.

## NOT Gate CMOS

How does CMOS work? When the voltage of input A is low A = 0, the upper transistor's channel is closed and we have a connection between Vdd(1) and Q, so Q = 1, this is a Pull Up Network. And when the voltage of input A is high, then the lower transistor's channel is closed and we have a connection between Vss(0) and Q, so Q = 0, this is a Pull Down Network. A question is raised – when does this circuit consume power? There is almost no power consume as there is no connection between Vdd and Vss at any time. Although when CMOS is switching between states, there is a minor power usage and we will see how we can use it for our purpose. Following is the NOT table:

| **input** | A | 0 | 1 |
|---|---|---|---|
| **output** | Not A | 1 | 0 |

Table 5.1: NOT gate truth table.

## AND Gate CMOS

Next we will see how to build a bit more complicated gate using 4 transistors. Following is the AND gate diagram:

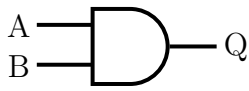


Figure 5.16: AND Gate.

We will implement the gate using 4 transistors to support the following AND table:

| **input a** | 0 | 0 | 1 | 1 |
|---|---|---|---|---|
| **input b** | 0 | 1 | 0 | 1 |
| **output** | 0 | 0 | 0 | 1 |

Table 5.2: AND gate truth table.

First we want to build the Pull Up Network, so for input A and B, for A=B=1 then the output Q is 1. Then we will build the Pull Down Network to support the other

combination from the table to deliver 0 as the output Q. Sometimes we don't want to have combination using the circuits, but we want to store information in it, next we will talk about another type of circuits called storage circuit or Sequential Circuit.

## Storage/Sequential Circuit

A latch or flip-flop is a circuit that has two stable states and can be used to store state information.

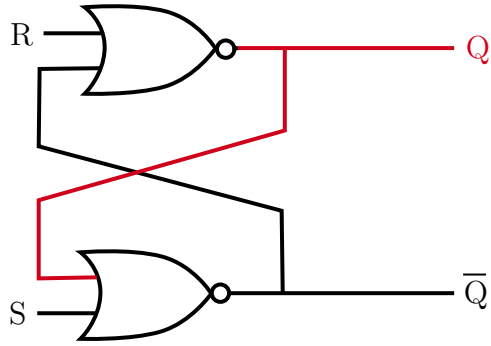


Figure 5.17: Flipflop.

The circuit can be made to change state by signals applied to one or more control inputs and will have one or two outputs. It is the basic storage element in sequential logic. Flip-flops and latches are fundamental building blocks of digital electronics systems used in comput-

ers, communications, and many other types of systems. A flip-flop is a device which stores a single bit (binary digit) of data; one of its two states represents a "one" and the other represents a "zero". Such data storage can be used for storage of state, and such a circuit is described as sequential logic in electronics. When used in a finite-state machine, the output and next state depend not only on its current input, but also on its current state (and hence, previous inputs). It can also be used for counting of pulses, and for synchronizing variably-timed input signals to some reference timing signal. Flip-flops can be either level-triggered (asynchronous, transparent or opaque) or edge-triggered (synchronous, or clocked). The term flip-flop has historically referred generically to both level-triggered and edge-triggered circuits that store a single bit of data using gates. We will refer Flip-Flop as edge-triggered i.e. clocked synchronized. Flip-flop has to legs – data and clock, for each storage element in the circuit the data changes at the clock signal and so we have an amplified signal that we can monitor as attackers and try to learn the secret behind it.

## Core I7 chip

Following is the core I7 chip image:

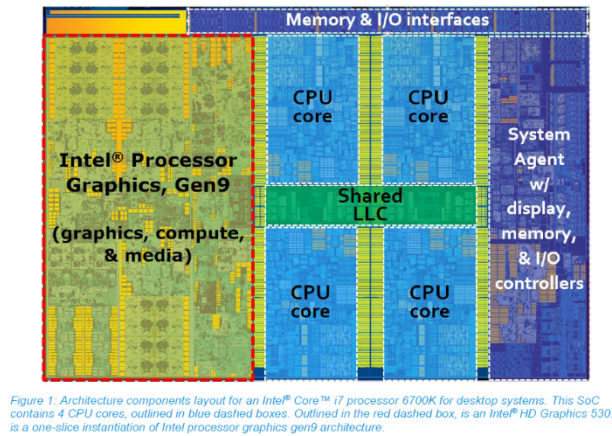


Figure 5.18: Intel i7.

We can see ordered items that are the storage elements, there are 24 items that are the GPUs and they have a little memory next to the (upper left). The CPU core has also a cash memory in it.

## Power Consumption is Variable

Next we will see how to get secrets from the power consumption.

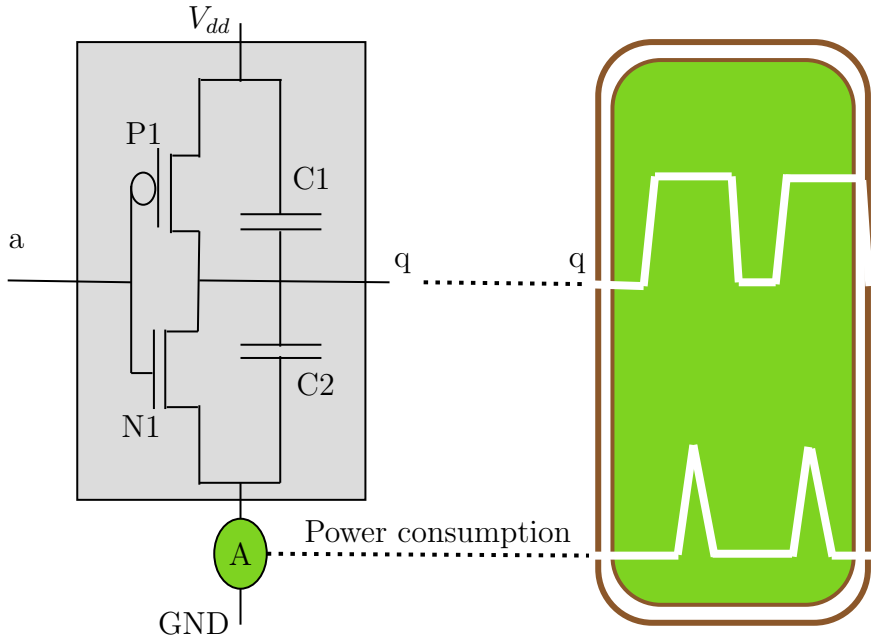


Figure 5.19: Not gate connected to an oscilloscope.

This is the NOT gate as before connected with an ampere meter so we can measure the power consumption,

also there are two capacitors (C1 & C2). The capacitors are connected because the characteristics of the circuit which make it to act like capacitors. They are not transferring current but they will have an effect on the math we are going to do next. Next we are taking a square wave, which looks like this: And we have to feed it into the NOT gates, the output is going to be the opposite of the square wave, and we want to measure the power consumption using an oscilloscope. The x axis of the oscilloscope is time and the y axis in this case it's a voltage of the power. It's a current moving across the ampere meter. What we can see here is that when the circuit is stable, there was not much power consumption, but when the system is switching, when there is a high power consumption, because there is a glitch when one transistor is opening and the other one is closing. Also, we can see that the lines in the oscilloscope are not having the same size as the capacitors are actually charging and discharging without we want it. We can learn from this if there was one or zero and what is the rate of switching, and we can store this information. The power consumption is the sum of the statistic and the dynamic power consumption:

$$P(t) = P_{stat}(t) + P_{dyn}(t)$$

We don't care about the statistic power consumption as it is just defined by the kind of silicone that we are using, the size of the features decided to be in the tran-

sistors, the temperature, the technology, etc. But really interesting for us is the dynamic power consumption that depends on the o'clock rate and the circuit activity input data. Because the power consumption is a function of the circuit activity, we can try to measure the power consumption and send the results to the equations and to get the circuit activity, in a way we can find out all the secrets. In order to calculate the power consumption this way we need a lots of data about the circuit and about the environment and about the temperature etc. And this is too much work for us as an engineers. There is a much simplified way of measuring the power consumption of a device, assuming it's a CMOS device we can measure how many bits changes every clock. So, our assumptions are the followings: 1. this is a CMOS device. 2. when it's static the static power is very low, and when it switches, there is a very high power consumption. 3. This is synchronous circuit, which means it has a lot of flip flops that all change at the same time. 4. The power consumption is proportional to the amount of changes and the outputs of these flip flops.

## hamming distance model

For doing this we are going to use hamming distance model. The Hamming distance between two vectors is the number of bits we must change to change one into the other. Example, what is the distance between the vec-

tors 01101010 and 11011011? Answer: They differ in four places, so the Hamming distance d(01101010,11011011) = 4. When talking about CMOS devices we are estimating our power consumption as amount of bits (transitions) that change from one to zero or from zero to one, this is our hamming distance. By monitoring the changes as explained we can find the power consumption. But, this is not enough. By connecting the oscilloscope to our device we are trying to measure a physical device with another physical equipment, and what they are measuring is subject to measurement errors like switching noise, thermal noise and measurement noises. Switching noise means that there are other kinds of activity which are going on in the circuit in addition. Measurement noise means that our desk setup is not always accurate, or we might be connected not properly, or we might not be measuring the precise correct moment of time etc. Thermal noise - we are measuring electrical activity, as electrons are very crazy particles and they like to disappear and reappear in a nearby location. So the higher is the temperature, the more likely they are to vanish and disappear. And when the electrons are moving, they generate radiation and they affect our measurements. So now when we are measuring the power, we get the static power, the dynamic power and we get the noise:

$$P_{meas}(t) = P_{stat}(t) + P_{dyn}(t) + N(t)$$

In order to avoid the noise we can measure it again and again and then the noise might be canceling itself. What happens sometimes is that the noise, especially the switching noise, is sometimes correlated with the activity of the circuits. Another thing we can do is controlling the noise somehow like running our experiment inside a freezer, or an isolated environment where there's no electric noise around. We can also, open the dives and try to kill the sources of noise. That's one very nice thing we can do is instead of measuring power consumption, we can measure electromagnetic radiation. And this has two advantages, first of all, it's less invasive and second of all, it can be focused and, and reduce the switching noise.

## From Power to Electromagnetic

Electric fields are created by differences in voltage: the higher the voltage, the stronger will be the resultant field. We can use the right hand rule in order to remember the direction of the electromagnetic field direction when we know the current direction. We can measure the magnetic field, but one disadvantage is that it is very localize, so we need to get access to the device. We can connect an antenna to the device and then we can measure the electromagnetic wave using a receiver. There is a very nice paper called screaming channels where you can read more about this kind of attacks.

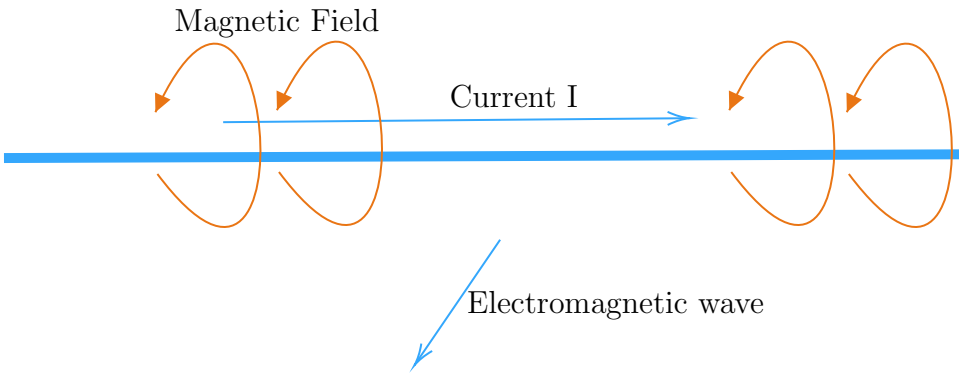


Figure 5.20: electromagnetic emition.

# Bibliography

[1] Clemens Lode. *Philosophy for Heroes: Knowledge.* Clemens Lode Verlag e.K., 2016.

[2] Clemens Lode. *Philosophy for Heroes: Continuum.* Clemens Lode Verlag e.K., 2017.